Create & Configure Service Principals

Step 1: Create a Service Principal in Azure Portal

1. **Login to Azure Portal**:
   - Navigate to Azure Portal and log in with your credentials.
2. **Go to Azure Active Directory**:
   - On the left-hand sidebar, select **Azure Active Directory** from the list of services.
3. **Register a New Application** (Service Principal):
   - Under the **Manage** section, select **App registrations**.
   - Click on **+ New registration**.
   - Fill in the details:
     - **Name**: Enter a name for your service principal (e.g., MyServicePrincipal).
     - **Supported account types**: Choose "Accounts in this organizational directory only (Default Directory only - Single tenant)".
     - **Redirect URI**: This is not mandatory for creating a service principal, so you can leave it blank.
   - Click **Register**.
4. **Generate a Client Secret**:
   - After registering the app, you will be redirected to the app's overview page.
   - In the left sidebar under **Manage**, click on **Certificates & secrets**.
   - Click **+ New client secret**.
   - Provide a description (e.g., MyClientSecret), and select an expiration duration (e.g., 1 year or 2 years).
   - Click **Add**.
   - Once the secret is created, **copy** the value shown. You **won't** be able to see it again after you navigate away from the page. This will be your **Client Secret**.
5. **Get the Client ID and Tenant ID**:
   - From the **Overview** page of your app registration:
     - **Application (client) ID**: This is your **Client ID**.
     - **Directory (tenant) ID**: This is your **Tenant ID**.
   - Copy these values for later.

6. **Assign Roles to the Service Principal**:
    - Now, you need to assign the service principal the necessary permissions to manage Azure resources.
    - Go to the **Subscription** (or **Resource Group**) where you want the service principal to have access.
        - In the left menu, click on **Access control (IAM)**.
        - Click **+ Add role assignment**.
        - In the **Role** dropdown, select the appropriate role (e.g., **Contributor**, **Owner**, **Reader** depending on the level of access required).
        - Under **Assign access to**, select **User, group, or service principal**.
        - Search for the **name** of the app (service principal) you created, select it, and click **Save**.

You've now created a service principal with permissions to manage resources in Azure.

Step 2: Add the Service Principal as a Service Connection in Azure DevOps

1. **Login to Azure DevOps**:
    - Go to Azure DevOps and sign in.
2. **Navigate to Your Project**:
    - Select the **project** where you want to add the service connection.
3. **Go to Project Settings**:
    - At the bottom left of the page, click on **Project settings**.
4. **Add a Service Connection**:
    - Under the **Pipelines** section, select **Service connections**.
    - Click **+ New service connection** at the top-right corner.
    - In the list of service connection types, select **Azure Resource Manager**.
    - Click **Next**.
5. **Choose Authentication Method**:
    - In the next screen, choose **Service principal (manual)**.
    - Click **Next**.
6. **Fill in the Service Principal Details**:
    - Enter the details of the service principal you created in Azure:

        - **Subscription ID**: You can find this in the **Subscriptions** section of the Azure portal or in the **Overview** section of your subscription.
        - **Subscription name**: The name of the subscription in Azure.
        - **Service Principal ID**: This is the **Application (client) ID** from Step 5 of the previous section.
        - **Service Principal Key**: This is the **Client Secret** you copied when creating the service principal.
        - **Tenant ID**: This is the **Directory (tenant) ID** from Step 5 of the previous section.

7. **Grant Access to All Pipelines** (Optional):
    - Optionally, you can check the box for **Grant access permission to all pipelines** to allow this service connection to be used in all pipelines within the project.
8. **Verify and Test**:
    - After entering all the details, click **Verify** to ensure that the service principal has the required access and the connection is correct.
9. **Save the Service Connection**:
    - Once verified, click **Save**.

Your service principal is now set up as a service connection in Azure DevOps, and you can use it in your pipelines to authenticate against Azure resources.
